AF | 2132 IFW

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	John B. Beavers		
Assignee:	Symantec Corporation		
Title:	SYSTEM AND METHOD FOR MANAGING ALERT INDICATIONS IN AN ENTERPRISE		
Serial No.:	10/082,235	Filed:	February 26, 2002
Examiner:	Venkatanaray Perungavoor	Group Art Unit:	2132
Docket No.:	SYMC1024		

Monterey, CA
June 2, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF

Dear Sir:

Pursuant to 37 CFR § 41.37(a)(1), Appellant files this Appellant's Brief in support of the Notice of Appeal filed on May 17, 2006.

Real Party in Interest

The assignee of the above-referenced patent application, Symantec Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

No other prior and pending appeals, judicial proceedings or interferences are known to appellant, the appellant's legal representative, or Assignee, which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1, 2, 4-10, 12-26 are pending in the application and stand rejected. The rejection of Claims 1, 2, 4-10, 12-26 is hereby appealed.

Claims 3, 11 have been canceled without prejudice.

Status of Amendments

All amendments have been entered. Applicant notes that no Amendments were filed after the final Office Action dated February 21, 2006.

Summary of Claimed Subject Matter

With respect to all of the independent Claims 1, 10, 23, referring to FIG. 3, Applicant's specification sets forth:

> First, **an alert indication is provided** at 21. (Page 9, line 6, emphasis added.)
>
> If no noise or unwanted information match is made at the filtering step 23, **the information is passed to the check rule step 27. This step analyzes input 21 to determine if** false positives are present, and whether a match at 28 exists for criteria and correlation set forth in the rules which will be described below. This step also causes memorization of patterns that may be emerging from the alert stream that do not immediately result in incident declarations but may result in same as further alerts are received, see box 36 in FIG. 3. **If a match is made, an incident is declared at step 29**. (Page 9, line 24 to page 10, line 9, emphasis added.)
>
> If no match is made at step 27, the input 21 is passed to a **Decision Table check step 31 wherein a decision table is used to determine** if false positives exist and whether a match exists between criteria in the Decision Tables and the input. **If such a match occurs at 32, an incident is declared at step 29**. (Page 10, lines 16-20, emphasis added.)
>
> If no match occurs, the input 21 is sent to a **default processing step 33. This step handles alert indications that may be considered serious but have no specific pattern that would be matched in the rule or decision table checking steps**. (Page 10, lines 21-24, emphasis added.)

Referring now to FIG. 4, Applicant's specification sets forth:

> **An incident ticket** can be associated with each incident declaration as shown in FIG. 4. **The ticket lists relevant details of the declared incident.** ... The header displays the incident ID, status, and priority or threat as displayed in the incident list. Therein, the highest priority conclusion is displayed followed by a listing of conclusions sorted by priority and age. Under the incident is a table of conclusions associated

> with the incident, followed by a list of actions taken. The tracking rule for the incident description is also shown as is a listing of the specific alert indications for each incident. The description contained under the alert heading corresponds to the input 21. (Page 13, lines 3-15, emphasis added.)
>
> The alert processing stream works in connection with incident ticket and its update tracking criteria feature. **This allows the addition of user tracking conditions to the automated tracking rule for the incident**. An example of a tracking rule is shown in FIG. 4 under the tracking rule heading. This displayed rule shows that if one of a number of a device, target or source IP's is identified, this alert is associated with the incident ticket. The incident tracking rule consists of a number of logical expressions joined by conjunctions, and display of a set of alert sources and targets that have been automatically detected by the system. (Page 28, line 9-19, emphasis added.)

Finally, referring now to FIGS. 4 and 6 together, Applicants' specification sets forth:

> **Using a pull down menu on the screen, a new rule can be written by the user** (as opposed to the default rule created by the automation when the incident was declared) **to apply to new alerts. Alert indications meeting the logic in the tracking criteria can then be associated with the incident ticket. FIG. 6 shows a typical updating screen 70, with the various input fields 71, 73, 75, and 77 as described above**. (Page 29, lines 1-7, emphasis added.)

Grounds of rejection to be reviewed on appeal

1. Whether Claims 1-2, 4-10, 12-26 are unpatentable under 35 U.S.C. 102(a) as being anticipated by Curtis et al. (6,208,720)?

Argument

1. Claims 1-2, 4-10, 12-26 are novel over Curtis et al. (6,208,720)

The Examiner states:

> Regarding Claim 1, Curtis discloses ... declaring an incident based on a threshold value see Fig. 4 item 414-416; and the **displaying of incident ticket including** a description of incident, a conclusion based on the ticket, any actions responsive to the conclusion, **one or more user editable incident tracking rules which identify the alert indications for association with the incident** and detail of the alert indications see Fig. 5C item 532, 534, 536 & Col 5 Ln 31-64. (Final Office Action dated Feb. 21, 2006, pages 2-3, emphasis added.)

The Examiner's statement is respectfully traversed. As set forth below, the Examiner has failed to callout where Curtis et al. teaches or suggests that an incident ticket is displayed, **the incident ticket itself including tracking rules that are editable by a user viewing the incident ticket.**

As set forth in the MPEP § 2131, eighth edition, Rev. 3, August 2005, at page 2100-76:

> TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM

Thus, although the Examiner asserts that Curtis et al. teaches "tracking rules", because the Examiner has failed to callout where Curtis et al. teaches or suggests that the **incident ticket itself including tracking rules that are editable by a user viewing the incident ticket, Claims 1-2, 4-10, 12-26 are novel over Curtis et al.**

Specifically, as set forth by the Applicant in the Amendment filed on January 27, 2006 at pages 11-13:

Regarding the "tracking rules" asserted by the Examiner, Curtis et al. teaches that the alarms are filtered and correlated by analysis layer 133.

Specifically, Curtis et al. teaches:

> Alarms which are generated by the detection layer 123 are sent to the analysis layer 133. **Analysis layer 133 analyzes alarm data and correlates different alarms which were generated from the same or related events and consolidates these alarms into fraud cases.** ... In a preferred embodiment, analysis layer 133 includes a software component 134 which performs the consolidation, correlation, and reduction functions. **Software component 134 uses external data from billing and AR systems 136 in the correlation and reduction processes.** Preferably, alarm database 138 resides on the same hardware as software component 134. (Col. 10, lines 32-62, emphasis added.)

Thus, Curtis et al. teaches that a software component 134 of analysis layer 133 uses external data from the billing and AR system 136 in the filtering and correlating of alarms. Accordingly, the Examiner has failed to callout where Curtis et al. teaches or suggests that an incident ticket is displayed, the incident ticket itself including tracking rules that are editable by a user viewing the incident ticket. Further, since Curtis et al. teaches that external data from the billing and AR system 136 is used in the filtering and correlating of alarms, Curtis et al. actually teaches away from an incident ticket that itself including tracking rules that are editable by a user viewing the incident ticket.

For at least the above reasons, Curtis et al. does not teach or suggest:

> A method of declaring an incident in an enterprise comprising:
>
> providing a number of alert indications containing information concerning an incident related to the enterprise; and either

> comparing one or more of the alert indications to a set of rules, and if a match occurs between the set of rules, and the alert indication, declaring an incident based on the match, or
>
> comparing one or more of the alert indications to a decision table containing a number of defined alert events; remembering each alert indication that matches one of the defined alert events, comparing the remembered alert indication to correlation data in the decision table, and if a match occurs between the remembered alert indication and the correlation data, declaring an incident based on the match; or
>
> if no match occurs between the alert indication and the correlation data or the rules set, declare an incident if the alert indication meets a defined default threshold value; and
>
> **displaying an incident ticket** for each incident declared, the incident ticket including a description of the incident, a conclusion based on the incident description, any actions responsive to the conclusion, **one or more user-editable incident tracking rules which identify one or more further alert indications for association with the incident ticket**, and a detail of the alert indications associated with the incident,

as recited in amended Claim 1, emphasis added. Accordingly, Claim 1 is allowable over Curtis et al. Claims 2, 4-9, 21-22, which depend from Claim 1, are allowable for at least the same reasons as Claim 1.

Claims 10 and 23 are allowable for reasons similar to Claim 1. Claims 12-20, which depend from Claim 10, are allowable for at least the same reasons as Claim 10. Claims 24-26, which depend from Claim 23, are allowable for at least the same reasons as Claim 23.

To further illustrate that the Examiner has failed to callout where Curtis et al. teaches or suggests that the incident ticket itself including tracking rules that are editable by a user viewing the incident ticket, regarding Claim 23, the Examiner states:

> ... a user uses an menu to change/update the alert indications see Col 28, Ln 26-33 & Col 15 Ln 29-36. And also see arguments above. (Final Office Action date February 21, 2006 at page 6.)

However, at Col. 15, lines 29-36 as cited by the Examiner, Curtis et al. teaches:

> Domain-specific implementation 1310 includes enhancement rules and configuration database 512 and a threshold detection rules database 522. **Databases 512 and 522 include rules which may be created, deleted or modified according to evolving needs of a user**. Changes to thresholding rules 522 may even be executed while the system is running. When a thresholding rule is created or modified, it will be applied to new events which arrive at the system. (Emphasis added.)

Although Curtis et al. teaches "rules which may be created, deleted or modified according to evolving needs of a user", the Examiner has failed to callout where Curtis et al. teaches or suggests that **the incident ticket itself including tracking rules that are editable by a user viewing the incident ticket.**

Finally, at Col. 28, Lines 26-42 as cited by the Examiner, Curtis et al. teaches:

> A presentation interface 1210 serves as an interface to workstations 152a . . . 152n, providing data for graphical presentation to the analyst. Fraud cases are presented according to presentation rules 1212, which are programmed as logical algorithms into a database and are configurable. **Presentation interface 1210 employs an informant 1214 and external systems 1216 to retrieve additional information.** However, this is not automatic, as in the upper layers. Rather informant 1214 retrieves data from external systems 1216 based on commands from analysts at work stations 152a . . . 152n. **For example, an analyst may view a case and decide that a customer's payment history is needed prior to taking any action. The analyst, via a workstation 152a . . . 152n, sends a command to presentation interface 1210 requesting this data. Presentation interface 1210 then instructs informant 1214 to retrieve this data from an external accounts receivable system 1216**. (Emphasis added.)

Accordingly, Curtis et al. teaches that an analyst may view a fraud case and request additional data. Again, the Examiner has failed to callout where Curtis et al. teaches or suggests that **the incident ticket itself including tracking rules that are editable by a user viewing the incident ticket.**

For at least these additional reasons, Curtis et al. does not teach or suggest:

> A method of declaring an incident in an enterprise comprising:
>
> providing a number of alert indications containing information concerning an incident related to the enterprise; and either
>
> comparing one or more of the alert indications to a set of rules, and if a match occurs between the set of rules, and the alert indication, declaring an incident based on the match, or
>
> comparing one or more of the alert indications to a decision table containing a number of defined alert events, remembering each alert indication that matches one of the defined alert events, comparing the remembered alert indication to correlation data in the decision table, and if a match occurs between the remembered alert indication and the correlation data, declaring an incident based on the match; or
>
> if no match occurs between the alert indication and the correlation data or the rules set, declare an incident if the alert indication meets a defined default threshold value;
>
> displaying to a user an incident ticket for each incident declared, **the incident ticket including one or more user-editable incident tracking rules which identify one or more further alert indications for association with the incident ticket;**
>
> **wherein the user uses a menu on the incident ticket to display a tracking update feature for editing the user-editable incident tracking rules;** and
>
> **wherein the user edits the user-editable** incident **tracking rules to change the one or more further alert indications for association with the incident ticket,**

as recited in Claim 23, emphasis added. Accordingly, Claim 23 is allowable over Curtis et al. Claims 24-26, which depend from Claim 23, are allowable for at least the same reasons as Claim 23.

Claims appendix

1. (Previously presented) A method of declaring an incident in an enterprise comprising:

providing a number of alert indications containing information concerning an incident related to the enterprise; and either

comparing one or more of the alert indications to a set of rules, and if a match occurs between the set of rules, and the alert indication, declaring an incident based on the match, or

comparing one or more of the alert indications to a decision table containing a number of defined alert events; remembering each alert indication that matches one of the defined alert events, comparing the remembered alert indication to correlation data in the decision table, and if a match occurs between the remembered alert indication and the correlation data, declaring an incident based on the match; or

if no match occurs between the alert indication and the correlation data or the rules set, declare an incident if the alert indication meets a defined default threshold value; and

displaying an incident ticket for each incident declared, the incident ticket including a description of the incident, a conclusion based on the incident description, any actions responsive to the conclusion, one or more user-editable incident tracking rules which identify one or more further alert indications for association with the incident ticket, and a detail of the alert indications associated with the incident.

2. (Original) The method of claim 1, wherein the defined default threshold value is a level of severity in the alert indication.

3. (Canceled)

4. (Previously presented) The method of claim 1, further comprising the step of tracking further alert indications once an incident ticket is declared and associating the further alert indications with the incident ticket based on the one or more user-editable incident tracking rules.

5. (Original) The method of claim 4, wherein the associating step is performed only if the further alert indications pass a threshold value or table lookup from a user-editable table which lists enterprise policy attributes associated with particular alert codes, categories, or threat characterizations.

6. (Previously presented) The method of claim 4, further comprising updating the one or more user-editable incident tracking rules based on one or more further alert indications.

7. (Original) The method of claim 1, wherein the alert indications include information having a common format.

8. (Original) The method of claim 1, wherein the enterprise is a network with a number of network devices that supply the alert indications for incident declaration.

9. (Original) The method of claim 1, wherein the default defined value derives from a set of rules defining default conditions for declaring an incident.

10. (Previously presented) A system for declaring an incident in an enterprise comprising:

a decision table containing a number of defined alert events, and a set of correlation data that identifies patterns in alert indications inputted to the decision table, the decision table remembering inputted alert indications matching defined alert events, and declaring an incident if a match occurs between remembered alert indications and the correlated data;

a set of rules containing a number of query statements, wherein a match between at least one of the rules and the inputted alert indications result in an incident declaration;

a set of default standards specifying a minimum value to declare an incident should a match not occur with the decision tables or set of rules; and a display of the incident as an incident ticket, the incident ticket including a description of the incident, a conclusion based on the incident description, any actions responsive to the conclusion, one or more user-editable incident tracking rules which identify one or more further alert indications for association with the incident ticket, a detail of the alert indications associated with the incident, followed by a listing of "raw events" that, if requested by the user, contains information that has been left in the native or vendor-specific format of the original sensor that produced the event.

11. (Canceled)

12. (Original) The system of claim 10, further comprising an alert processing system that tracks inputted alert indications, filters out inputted alert indications that do not meet a threshold value, compares the inputted information to a tracking rule to determine whether the inputted information should be associated with a declared incident.

13. (Original) The system of claim 10, further comprising a database for storing at least the declared incidents.

14. (Original) The system of claim 12, further comprising a database for storing at least the declared incidents and alert indications passing the threshold value.

15. (Original) The system of claim 13, further comprising a web server, linking the system to one or more users via a global network.

16. (Original) The system of claim 10, further comprising means for displaying the declared incident.

17. (Original) The system of claim 10, wherein the rules are a combination of default rules and customized rules.

18. (Original) The system of claim 10, wherein the enterprise is a network and the inputted information is supplied by a number of network devices.

19. (Original) The system of claim 12, further comprising an alert processing system that tracks inputted alert indications, filters out inputted alert indications that do not meet a threshold value, compares the inputted information to a tracking rule to determine whether the inputted information should be associated with a declared incident.

20. (Original) The system of claim 19, wherein the enterprise is a network, and the inputted information is supplied by a number of network devices.

21. (Previously presented) The method of claim 1, comprising updating the incident ticket based on an updated tracking rule such that the alert indications, conclusions and description reflect the updated tracking rule.

22. (Original) The method of claim 21, wherein the tracking rule is updated using human input based on observations of reported incidents.

23. (Previously presented) A method of declaring an incident in an enterprise comprising:

providing a number of alert indications containing information concerning an incident related to the enterprise; and either

comparing one or more of the alert indications to a set of rules, and if a match occurs between the set of rules, and the alert indication, declaring an incident based on the match, or

comparing one or more of the alert indications to a decision table containing a number of defined alert events, remembering each alert indication that matches one of the defined alert events, comparing the remembered alert indication to correlation data in the decision table, and if a match occurs between the remembered alert indication and the correlation data, declaring an incident based on the match; or

if no match occurs between the alert indication and the correlation data or the rules set, declare an incident if the alert indication meets a defined default threshold value;

displaying to a user an incident ticket for each incident declared, the incident ticket including one or more user-editable incident tracking rules which identify one or more further alert indications for association with the incident ticket;

wherein the user uses a menu on the incident ticket to display a tracking update feature for editing the user-editable incident tracking rules; and

wherein the user edits the user-editable incident tracking rules to change the one or more further alert indications for association with the incident ticket.

24. (Previously presented) The method of claim 23 wherein the user-editable tracking rules include a source IP address, at least one target IP address, a conjunction, an attribute name, a condition, and an attribute value.

25. (Previously presented) The method of claim 23 wherein the information contained in the alert indications relates to an unauthorized access attempt into the enterprise.

26. (Previously presented) The method of claim 25 wherein the information contained in the alert indications relates to a port scan.

Evidence appendix

None

Related proceedings appendix

None

Conclusion

If there are any questions relating to the above, please telephone the undersigned Attorney for Applicant.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 2, 2006.

Attorney for Applicant(s)

June 2, 2006
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880

GUNNISON, McKAY & HODGSON, L.L.P.
GARDEN WEST OFFICE PLAZA, SUITE 220
1900 GARDEN ROAD
MONTEREY, CALIFORNIA 93940
(831) 655-0880
FACSIMILE (831) 655-0888

June 2, 2006

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

RE:	Applicant(s):	John B. Beavers		
	Assignee:	Symantec Corporation		
	Title:	SYSTEM AND METHOD FOR MANAGING ALERT INDICATIONS IN AN ENTERPRISE		
	Serial No.:	10/082,235	Filed:	February 26, 2002
	Examiner:	Venkatanaray Perungavoor	Group Art Unit:	2132
	Docket No.:	SYMC1024		

Dear Sir:

Transmitted herewith are the following documents in support of the Notice of Appeal filed on May 17, 2006 in the above application:

1. Return receipt postcard;
2. Check in the amount of $500.00 for filing a brief in support of an appeal;
3. This Transmittal Letter (2 pages); and
4. Appellant's Brief (25 pages).

☒ Conditional Petition for Extension of Time: If an extension of time is required for timely filing of the enclosed documents after all papers filed with this transmittal have been considered, Applicant(s) hereby petition for such an extension of time.

☒ The Commissioner is hereby authorized to charge any additional fees required for consideration of the enclosed documents, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on June 2, 2006.

Attorney for Applicant(s)

June 2, 2006
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017